



Document Summary



New
Search



Help

[Preview Claims](#)

[Preview Full Text](#)

[Preview Full Image](#)

Email Link:

Document EP 0 552 078 A1

ID:

Title: INSERTABLE CARD FOR MICROCOMPUTER CONSTITUTING A READER FOR CARDS WITH FLAT CONTACTS

Assignee: Gemplus Card International S.A.

Inventor: LEROUX, JEAN-YVES

US Class:

Int'l Class: [5] G06F 12/06 A; G06K 19/06 B; G06K 7/06 B

Issue Date: 07/21/1993

Filing Date: 01/08/1993

Abstract:

The invention relates to removable memory cards with several integrated circuits, for personal computers. These memory cards serve as a large-capacity mass memory intended to replace the diskettes and other removable magnetic media. They have a plug-in connector (12) at the end of the card and can be inserted into the reader to the PCMCIA standards of a microcomputer. According to the invention, it is proposed to make up a chip card reader with flush contacts from such a plug-in card (10). In order to do that, the card (10) includes an additional connector with flush contacts on its main face (14). The reader thus produced is transportable, with its application software stored in the card (10) onto no matter what microcomputer equipped with a PCMCIA reader. A credit card or security card (18) may then be inserted into this transportable reader.

§ PAGE BLANK (USPTO)



DEMANDE DE BREVET EUROPEEN

Numéro de dépôt : 93400040.7

Int. Cl.⁵ : **G06F 12/06, G06K 19/06,
G06K 7/06**

Date de dépôt : 08.01.93

Priorité : 14.01.92 FR 9200323

Date de publication de la demande :
21.07.93 Bulletin 93/29

Etats contractants désignés :
DE ES GB IT NL

Demandeur : **GEMPLUS CARD
INTERNATIONAL S.A.**
Avenue du Pic de Bertagne, Zone d'Activités
de la Plaine de Jouques
F-13420 Gemenos (FR)

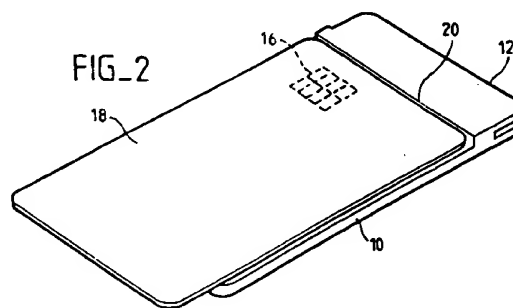
Inventeur : **Leroux, Jean-Yves**
Cabinet Ballot-Schmit, 7, rue Le Sueur
F-75116 Paris (FR)

Mandataire : **Schmit, Christian Norbert Marie
et al**
Cabinet Ballot-Schmit 7, rue Le Sueur
F-75116 Paris (FR)

Carte enfichable pour microordinateur formant lecteur de carte à contacts affleurants.

L'invention concerne les cartes à mémoire amovibles à plusieurs circuits-intégrés, pour ordinateurs personnels.

Ces cartes à mémoire servent de mémoire de masse de grande capacité destinées à remplacer les disquettes et autres supports magnétiques amovibles. Elles ont un connecteur enfichable (12) en bout de carte et peuvent être insérées dans le lecteur aux normes PCMCIA d'un microordinateur. Selon l'invention, on propose de constituer un lecteur de cartes à puces à contacts affleurants à partir d'une telle carte enfichable (10). Pour cela, la carte (10) comporte un connecteur supplémentaire à contacts affleurants sur sa face principale (14). Le lecteur ainsi réalisé est transportable, avec ses logiciels d'application stockés dans la carte (10), sur n'importe quel microordinateur équipé d'un lecteur PCMCIA. Une carte de crédit ou carte de sécurité (18) peut alors être insérée dans ce lecteur transportable.



EP 0 552 078 A1

sous le contrôle de la carte de crédit. La carte de crédit peut être une carte d'habilitation (carte de sécurité) autorisant l'usage du microordinateur.

Dans le premier aspect de cette invention, la carte à mémoire 10 a pour fonction principale de constituer un lecteur de carte à contacts affleurants, ce lecteur étant amovible par nature, de la même manière qu'une disquette magnétique est amovible. Dans ce cas, les mémoires et autres puces de circuit intégré de la carte sont dédiés à cet usage, c'est-à-dire que la carte comporte par exemple un microprocesseur qui gère les protocoles de communication avec le connecteur 16 et des mémoires contenant les programmes de fonctionnement de ce microprocesseur et les programmes d'interfaçage avec l'ordinateur par le connecteur 12.

Dans un autre aspect de l'invention, étant donné les capacités de mémoire et de traitement élevées des cartes PCMCIA, la circuiterie servant à transformer la carte 10 en lecteur de cartes à contacts affleurants n'est qu'un aspect auxiliaire du fonctionnement de la carte à mémoire. La carte possède des fonctions principales destinées à être accomplies sous contrôle de l'ordinateur, et la fonction de lecteur de carte de crédit est une fonction parmi ces fonctions:

Pour terminer cette description, on va montrer comment l'invention peut servir tout particulièrement dans ce dernier cas à assurer la protection du contenu de la carte à mémoire de masse elle-même.

Selon un aspect de l'invention, on a en effet pensé qu'il serait souhaitable de sécuriser autant que possible les cartes à mémoire de masse pour microordinateurs personnels. En effet, leur grande capacité fait qu'elles peuvent contenir soit des bases de données importantes méritant d'être protégées en lecture comme en écriture, soit des programmes coûteux qu'on ne souhaite pas voir utiliser ou dupliquer sans autorisation; ou enfin, elles peuvent servir à assurer des transactions confidentielles selon des programmes plus sophistiqués que ceux qui existent actuellement, ou impliquant des quantités de données plus importantes que ce que peuvent stocker les simples cartes à puces de transactions sécurisées qui ne comportent qu'une puce.

Par conséquent, on pourra prévoir, avec la structure selon l'invention, que la carte à mémoire de masse comporte des programmes de gestion de sécurité; ces programmes interdisent l'utilisation de la carte à mémoire si d'une part une carte de sécurité à contacts affleurants n'est pas présente dans le lecteur de carte en même temps que la carte à mémoire, et si d'autre part le dialogue entre la carte à mémoire, la carte de sécurité, et l'utilisateur du microordinateur, fait apparaître que l'utilisateur n'est pas le titulaire habilité de la carte de sécurité correspondant à ce que la carte à mémoire attend. Par l'expression "carte de sécurité", on entend ici une carte apte à vérifier une habilitation ou à crypter des données d'une manière

impossible ou quasi-impossible à frauder. Une carte contenant un code confidentiel et des moyens de vérification du code introduit au clavier par l'utilisateur est un exemple de carte de sécurité.

Par conséquent, on peut grâce à l'invention imaginer le protocole de fonctionnement suivant : une carte à mémoire est insérée dans le lecteur du microordinateur; cette opération déclenche un protocole de communication permettant au microordinateur de dialoguer partiellement avec la carte; l'insertion d'une carte de sécurité est demandée à l'écran; si une carte de sécurité n'est pas introduite, l'utilisation normale de la carte à mémoire ne sera pas possible; si une carte de sécurité est introduite, un dialogue s'établit entre celle-ci et la carte à mémoire, cette dernière contrôlant la situation; un mot de passe est demandé à l'écran; le mot de passe est introduit par l'utilisateur au clavier; ce mot de passe est reçu par la carte à mémoire qui le transmet directement, ou mieux encore sous forme chiffrée, à la carte de sécurité; celle-ci exécute les opérations de vérification nécessaires sur le mot de passe; si le mot de passe n'est pas correct, le signal renvoyé par la carte de sécurité est lu par la carte à mémoire comme une interdiction de fonctionnement normal; elle bloque donc les parties de circuits ou de mémoires qui doivent rester protégées; l'autorisation de fonctionnement normal de la carte n'est pas donnée par la carte au PC : la carte se protège elle-même contre une utilisation non autorisée; si le mot de passe est correct, l'autorisation est donnée. L'autorisation peut être générale une fois que le mot de passe a été donné, ou peut être partielle selon le degré d'habilitation auquel donne droit le mot de passe.

On voit qu'une protection sophistiquée peut être obtenue sur le contenu de la carte : d'une part on peut protéger tout ou partie de la carte, en lecture comme en écriture; d'autre part, le fabricant de carte peut prévoir qu'il y a correspondance entre la carte à mémoire et une carte de sécurité spécifique associée; dans ce dernier cas, le fonctionnement de la carte peut n'être autorisé que si non seulement l'utilisateur possède un mot de passe mais aussi si la carte de sécurité est bien celle qui est attendue; on peut prévoir aussi une habilitation si une seule de ces conditions seulement est remplie.

On aura compris que la carte à mémoire est protégée sans que le dialogue de vérification de la sécurité passé par le microordinateur, ce qui est avantageux.

On a ainsi donné un exemple particulièrement important de l'utilisation qu'on peut faire de l'invention. Jusqu'à maintenant les cartes à mémoire de masse ne pouvaient pas être protégées, et seuls les microordinateurs pouvaient être protégés globalement, sans que leurs différents lecteurs de mémoires de masse puissent être protégés individuellement, et surtout sans que les contenus de ces mémoires de

masse puissent être protégés dès lors qu'elles étaient insérées dans un microordinateur non protégé.

Le circuit intégré qu'on insère dans une telle carte de sécurité est de préférence une puce unique comportant une mémoire non volatile avec des informations confidentielles qui ne peuvent pas être transmises sur les bornes extérieures du circuit-intégré, et une circuiterie de sécurité programmée; cette circuiterie est apte à utiliser ces informations confidentielles et d'autres informations fournies par l'utilisateur, pour délivrer des instructions de validation après vérification d'une relation prédéterminée entre ces deux types d'information; les données confidentielles ne sortent pas à l'extérieur du circuit intégré.

La puce de sécurité comporte elle-même éventuellement un microprocesseur et des mémoires, avec parmi ces mémoires des mémoires non volatiles programmables électriquement et éventuellement effaçables électriquement. Le programme de fonctionnement de ce microprocesseur est en principe enregistré dans une mémoire morte de la puce; mais il peut être également partiellement enregistré dans une mémoire non volatile. Le contenu de certaines au moins des mémoires non volatiles n'est pas accessible en lecture sur les bornes extérieures de la puce. Ce contenu est utilisé exclusivement par le microprocesseur pour ses besoins propres, et notamment pour l'exécution de programmes de sécurité faisant intervenir des codes secrets placés dans ces mémoires inaccessibles. A titre d'exemple, le circuit intégré ST16612 vendu par SGS-THOMSON, auquel est incorporé le programme de mémoire non volatile MCOS de GEMPLUS, peut convenir.

Dans un autre exemple la carte de crédit est d'un format plus petit, par exemple au format dit PLUG-IN, défini pour l'utilisation en Téléphonie Cellulaire Européenne (norme G.S.M.). Dans ce cas la carte à mémoire où au moins son support 10 ne comporte qu'une cavité de dimension adaptée, de préférence là où une puce mémoire n'a pas été placée. Cette cavité ne possède qu'une ouverture supérieure. Elle ne débouche pas à l'arrière de la carte à mémoire. Cette cavité est munie dans son fond d'un connecteur pour venir au contact des métallisations de la carte PLUG-IN qui y est placée. Un autre avantage de cette solution est que son intégration la rend plus solide, en particulier parce que la carte ne déborde pas. L'arrachement de la carte à puce PLUG-IN est en effet impossible sans arracher la carte à mémoire elle-même. Ceci empêche toute violation, l'application s'arrêtant immédiatement si celle-ci est retirée. De plus, l'espionnage des contacts de la carte à puce devient quasiment impossible.

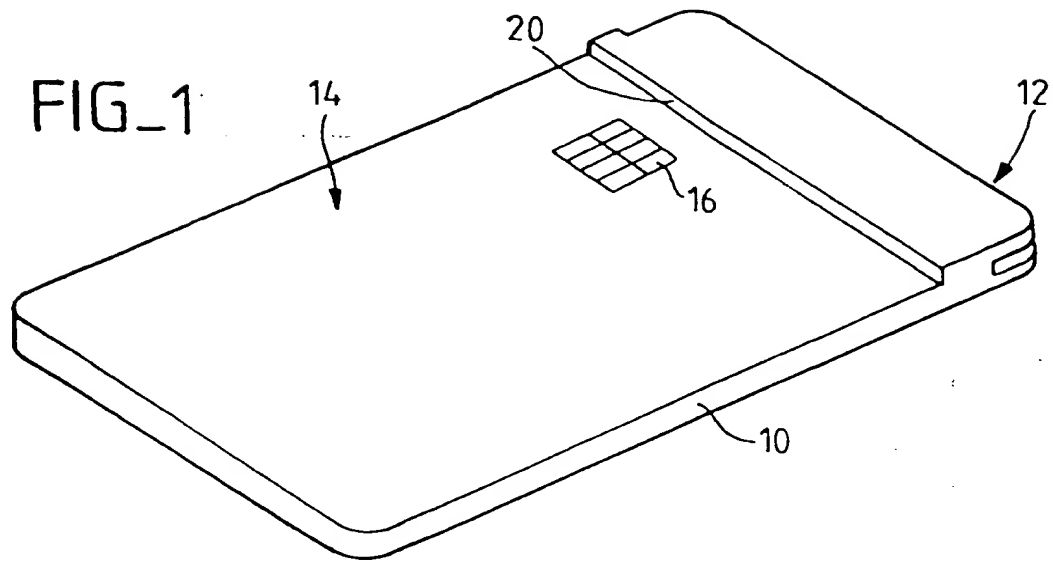
Revendications

1. Carte à mémoire enfichable (10) pour microordi-

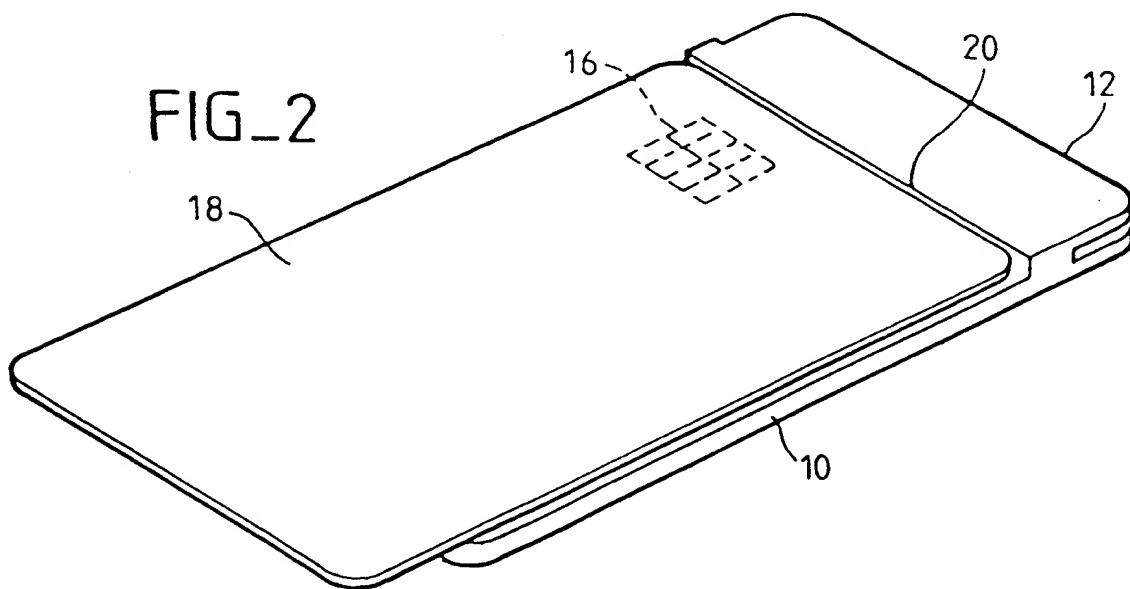
nateur, comportant plusieurs puces de circuit-intégré et un connecteur (12) à plusieurs dizaines de contacts enfichables en bout de carte, caractérisée en ce qu'elle comporte en outre un connecteur supplémentaire (16) à quelques contacts affleurants sur une surface principale (14) de la carte, ce connecteur supplémentaire étant apte à venir en contact avec une carte à puce (18) plane dont les contacts d'accès affleurent sur une face principale.

2. Carte à mémoire enfichable pour microordinateur, selon la revendication 1, caractérisée en ce que le connecteur supplémentaire a des contacts légèrement en saillie par rapport à la surface principale (14) de la carte enfichable.
3. Carte à mémoire enfichable selon l'une des revendications 1 et 2, caractérisée en ce qu'elle comporte des moyens électroniques pour dialoguer avec une carte de sécurité à contacts affleurants placée en contact avec le connecteur supplémentaire, et des moyens pour protéger l'accès à la carte enfichable à partir d'un ordinateur dans lequel elle est enfichée, en fonction des résultats du dialogue.
4. Carte à mémoire selon l'une des revendications 1 à 3 caractérisée en ce qu'elle est enfichée dans un réceptacle qui comporte des flancs latéraux pour guider en même temps la carte à mémoire et la carte à puce.
5. Carte à mémoire selon l'une quelconque des revendications 1 à 4 caractérisée en ce qu'elle comporte une cavité pour recevoir une carte à puce de dimension réduite.

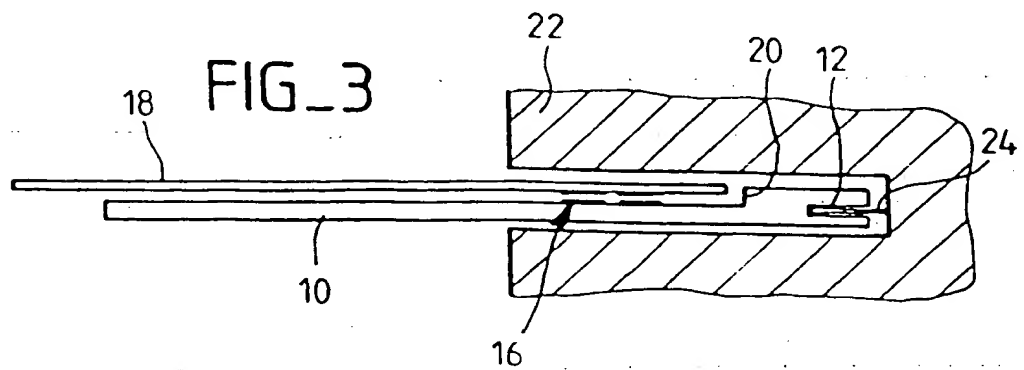
FIG_1



FIG_2



FIG_3



Office européen
des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numero de la demande

EP 93 40 0040

DOCUMENTS CONSIDERES COMME PERTINENTS			
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int. Cl.5)
Y	FR-A-2 637 749 (ELECTRONIQUE SERGE DASSAULT) * abrégé * * page 5, ligne 26 - page 6, ligne 22 * * page 7, ligne 22 - ligne 33 * * page 8, ligne 11 - ligne 20 * * figures 1,2 * ---	1,2	G06F12/06 G06K19/06 G06K7/06
Y	ELEKTRONIK. vol. 37, no. 17, 19 Août 1988, MUNCHEN DE pages 42 - 43 'Viel Leistung - wenig Platz' * page 42, colonne 1, ligne 1 - ligne 13 * * page 42, colonne 4, ligne 14 - page 43, colonne 1, ligne 2 * * page 43, colonne 4, ligne 12 - ligne 38 * * figures 1,4 * ---	1,2	
Y A	EP-A-0 323 347 (SCHLUMBERGER INDUSTRIES) * colonne 2, ligne 53 - colonne 3, ligne 58 * * figures 1,2 * ---	2 1	DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5) G06F G06K
A	EP-A-0 328 124 (DEUTSCHE BUNDESPOST) * le document en entier * ---	1,5	
A	EP-A-0 402 182 (PARIENTI, RAOUL) * le document en entier * -----	1	
Le présent rapport a été établi pour toutes les revendications			
Lieu de la recherche BERLIN		Date d'achèvement de la recherche 19 AVRIL 1993	Examineur MASCHE C.
<p>CATEGORIE DES DOCUMENTS CITES</p> <p>X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire</p> <p>T : théorie ou principe à la base de l'invention E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date D : cité dans la demande L : cité pour d'autres raisons Δ : membre de la même famille, document correspondant</p>			

EPO FORM 1500 (01.92) (page 2)

THIS PAGE BLANK (USPTO)